(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/027597 A3

(51) International Patent Classification[7]: G06F 7/72

(21) International Application Number:
PCT/IB2003/003949

(22) International Filing Date:
10 September 2003 (10.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0221837.8 20 September 2002 (20.09.2002) GB

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HUBERT, Gerardus, T., M. [NL/NL]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

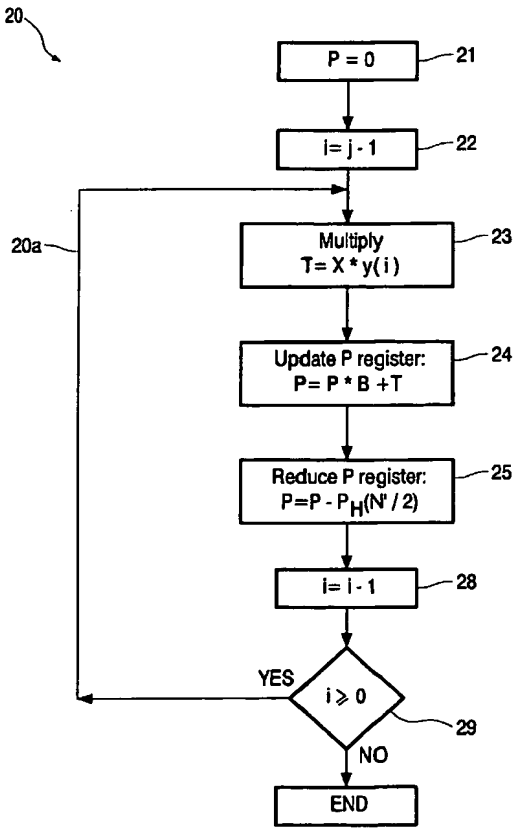
(74) Agent: TURNER, Richard, C.; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: QUISQUATER REDUCTION



(57) Abstract: A method and apparatus for calculating the product P of a first number X and a second number Y, modulo N, where Y is partitioned into j words each of length p bits, and has a length (m + n) bits, cyclically operates on successive ones of the j words of Y, carrying out intermediate modulo reductions of the intermediate products formed. A specially selected multiple, N', of N is used so that only a single reduction of the intermediate based on N' guarantees that the intermediate product P is never longer than (m+n) bits at the end of each cycle. N' is an integer multiple of N, and the value N' is selected such that the (m - 1) most significant bits are equal to '1', and the least significant bit is '0'.

WO 2004/027597 A3

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
11 November 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

International Application No
:T/IB 03/03949

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 366 673 B1 (VAN DIJK MARTEN E ET AL) 2 April 2002 (2002-04-02) abstract column 3, line 1 - column 6, line 9	1-15
A	ORTON G ET AL: "A DESIGN OF A FAST PIPELINED MODULAR MULTIPLIER BASED ON A DIMINISHED-RADIX ALGORITHM" JOURNAL OF CRYPTOLOGY, NEW YORK, NY, US, vol. 5, 1992, pages 183-208, XP000669945 abstract figures 1,4	1-15
A	DE 101 42 155 C (INFINEON TECHNOLOGIES AG) 23 May 2002 (2002-05-23) abstract page 6, line 59 - page 7, line 37 page 8, line 15 - page 9, line 52 figures 4-7	1-15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 September 2004	04/10/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6366673	B1	02-04-2002	EP	0938790 A2	01-09-1999
			WO	9914880 A2	25-03-1999
			JP	2001505325 T	17-04-2001
DE 10142155	C	23-05-2002	DE	10142155 C1	23-05-2002
			WO	03021424 A2	13-03-2003
			EP	1421474 A2	26-05-2004